VZCZCXYZ0001
OO RUEHWEB

DE RUEHKO #4801/01 2880005
ZNY CCCCC ZZH
O 150005Z OCT 07
FM AMEMBASSY TOKYO
TO RUEHC/SECSTATE WASHDC IMMEDIATE 8548
RUEKJCS/SECDEF WASHDC IMMEDIATE
INFO RHEHAAA/NSC WASHDC
RUENAAA/CNO WASHINGTON DC
RUEKJCS/CJCS WASHINGTON DC
RUYNAAC/COMNAVFORJAPAN YOKOSUKA JA
RUEAIIA/CIA WASHDC
RHMFISS/USFJ
RHEFDIA/DIA WASHINGTON DC
RHHMUNA/HQ USPACOM HONOLULU HI
RUEKJCS/JOINT STAFF WASHINGTON DC
RUEHKO/USDAO TOKYO JA

C O N F I D E N T I A L TOKYO 004801

SIPDIS

SIPDIS

OSD FOR APSA SHINN/SEDNEY/HILL/BASALLA; USFJ FOR
J00/J01/J2/J5

E.O. 12958: DECL: 10/12/2017
TAGS: PREL PGOV PINR MARR JA
SUBJECT: BILATERAL INFORMATION SECURITY TASK FORCE ADVANCES
TERMS OF REFERENCE MILESTONES ON INFORMATION SECURITY

REF: TOKYO 3690

Classified By: CDA Joseph R. Donovan, Reasons: 1.4 (b/d)

¶1. (C) The DAS-level U.S.-Japan Bilateral Information
Security Task Force (BISTF) and the Tokyo-based
Implementation Group (IG) have made steady progress on
implementing milestones agreed upon bilaterally on August
¶3. The BISTF process is divided into three broad phases.
The first aims to enhance mutual understanding of existing
information security laws and policies. The second phase
involves a bilateral process to administratively correct
information security practices identified during a series
of information exchanges. The contents of the final stage,
enhancing the legal framework for protecting classified
information, are still subject to "refinement" by the two
sides. While Japan has agreed in principal to discuss
"visionary" objectives like new legislation governing
security clearances, the Japanese government is reluctant
to commit to a timetable given political variables. This
cable chronicles progress made to date on implementing
near-term objectives and formulating a way forward on
future actions. The Terms of Reference and Milestones
document can be accessed from SIPR site
http://www.intelink.sgov.gov/wiki/Bilateral_I nformation_Secu
rity_Task_Force. END SUMMARY.

BACKGROUND

¶2. (C) On August 1 and 3, U.S. and Japanese DAS-level
officials convened the first Bilateral Information Security
Task Force (BISTF) meeting in Tokyo to approve the Terms of
Reference (TOR) and Milestones aimed at strengthening
Japan's ability to protect classified information
(reftel). Subsequent to the TOR's approval, the
Tokyo-based BISTF Implementation Group (IG) has convened
numerous meetings between August 16 and September 14 to
advance and refine near- and mid-term milestones in the
run-up to the second DAS-level meeting, held September 19
in Washington. The IG comprises Embassy and USFJ officers
and Director-level officials from the Ministry of Foreign
Affairs (MOFA), the Ministry of Defense (MOD), the Cabinet
Secretariat, the Cabinet Intelligence and Research Office

SIPDIS
(CIRO), the National Police Agency (NPA), and the Public Security Intelligence Agency (PSIA).

AUG 21 IG: INFO/BEST PRACTICES BRIEFINGS

¶3. (C) The first BISTF Implementation Group (IG) plenary meeting convened on August 21 with information and best practices briefings from both sides. The U.S. briefings also included discussion on establishing secure links between the Embassy and relevant ministries and agencies, reciprocal visit/surveys under the recently signed General Secrets of Military Information Agreement (GSOMIA),

SIPDIS
transferring pre-packaged security materials per Foreign Military Sales, and enhancing DOD's Foreign Visit System. Embassy and USFJ staff also provided briefings on Security of Diplomatic Information and Communications, Threats to Cybersecurity, Personnel Security Clearances and Access, Courier Procedures, Government-to-Industry Transfer of Classified Information, and Physical Security.

JAPAN'S NEW COUNTER-INTELLIGENCE POLICY

¶4. (C) Counselor Yuji Kawabe from the Cabinet Intelligence and Research Office (CIRO) explained Japan's new counter-intelligence (CI) policy, which the Japanese Cabinet approved on August 10. Under the new framework, the head of each government agency will classify national security and diplomatic information as "Specially Controlled Secret" beginning April 1, 2009. The new policy requires government agencies to make infrastructure upgrades for protecting classified information, as well as procedural upgrades, including security clearances and

training. It establishes, for the first time, a government-wide security clearance system. The new policy also provides the basis for the establishment of the National Counter-intelligence Center (NCC), Kawabe said. The NCC, to be established in April 2008, will collect and analyze counter-intelligence data for reporting to the Cabinet and relevant ministries and agencies. The center will support the CI Driving Committee and act as liaison and coordination body for CI policy implementation.

LAUNCH OF MOFA'S COUNTER-INTELLIGENCE DIVISION

¶5. (C) The Japanese side cited the Ministry of Foreign Affairs as among the first Japanese government agencies to establish an in-house CI division consistent with the new policy. The newly-established MOFA Counter-Intelligence Division is part of the Minister's Secretariat and reports directly to the Deputy Vice Minister (Kanbocho), according to CI Division Director Hitoshi Noda. Established on August 10, the ten-person division is responsible for planning and implementing the Japanese government's new CI policy throughout MOFA, specifically on protecting classified information at MOFA headquarters and at overseas missions. The division is also responsible for refining MOFA's security clearance system, enhancing physical information security (i.e., technical security), and improving infrastructure.

AUG 30 PLENARY: GOJ RESISTS SINGLE POC IDEA

¶6. (C) The second BISTF IG plenary session on August 30 centered on designating single points of contact for incidents involving classified information and standing up working groups and action groups for information and best practices briefings. The U.S. proposed designating a single POC to make initial notifications of a breach.

¶7. (C) The Japanese side subsequently provided a compromise approach on the single POC concept, comprising of two parts: first, how incidents are reported from the U.S. side to the Japanese side in cases involving classified military information (CMI) under the GSOMIA; second, all other cases. Under the Japanese proposal, the Embassy's Defense Attache would inform MOFA's Japan-U.S. Security Treaty Division Director, who would subsequently inform the Cabinet Secretariat, CIRO, MOD, NPA, and PSIA. The Japanese side stressed that the procedure only applied to initial notification of an incident, not the substance of the compromised information or any investigatory details. The process also does not supplant existing lines of communication, which the two sides would use in all non-CMI, non-GSOMIA cases.

WORKING GROUPS AND ACTION GROUPS

¶8. (C) At the August 30 meeting, the two sides also agreed to establish two working groups and three action groups to bring together relevant subject matter experts. The working groups and action groups would convene sometime after the September 19 BISTF meeting in Washington, covering the following topics:

-- Working group 1: personnel security clearance, cybersecurity, physical security

-- Working group 2: security of diplomatic info/communications, courier procedures

-- Action group 1: development of AEGIS security plan

-- Action group 2: development of CI ramifications and lessons learned from AEGIS compromise

--Action group 3: secured links

The working groups and action groups would each have U.S. and Japanese co-chairs, who will report the results of their meetings at the IG plenary.

SEP 14 IG: PREPARING FOR PLENARY

¶9. (C) The third IG meeting on September 14 centered on four items: the agenda for the September 19 DAS-level BISTF plenary meeting in Washington, single points of contacts for incidents involving classified information, target completion dates for the TOR mid-term milestones, and a briefing from the Japanese side on their military officer-journalist exchange program. The Japanese side underscored repeatedly that the goal of the September 19 BISTF meeting was to have substantive discussions on "refining" the long-term milestones, not necessarily reaching final agreement on them. They proposed that the BISTF plenary adhere to the exact wording of the TOR, which stipulates the long-term milestones "will be refined bilaterally at the second BISTF meeting."

SEP 19 WASHINGTON PLENARY

¶10. (C) The second DAS-level BISTF plenary meeting convened on September 19 in Washington, with substantive discussion on all the milestones. Both sides delegated a number of tasks to the Tokyo-based IG. First, the task force added one new near-term milestone, which states that the Tokyo-based IG will prepare a joint status assessment for all near-term milestones to be presented at the next BISTF plenary, to be held in Tokyo on November 13. Second, the group agreed that the IG will determine a new target date for the draft damage assessment of the AEGIS compromise, considering that ongoing criminal investigations made completion by the original target date of October 20 impossible. Third, the IG will continue discussions on the U.S. proposal on developing an Information Sharing

Roadmap. The Japanese delegation added that it will take additional time to coordinate the U.S. proposal with Japanese ministries not represented in BISTF, such as the Ministry of Economics, Trade and Industry (METI). Finally, both delegations agreed to continue discussions on the intent and wording of the long-term milestones at the IG level, along with the addition of "cyber forensics" to the list of topics.

SOME TARGET DATES EXTENDED

¶11. (C) The two delegations altered the target dates on a number of mid-term milestones after assessing both sides' logistic needs and domestic political situations. For example, the reciprocal visits by survey teams under the GSOMIA, which had a target date of October 31, was adjusted to allow for a proposed trip by the National Disclosure Policy Committee (NDPC) to Japan will have sufficient time to translate and review Japanese laws and regulations for the handling of classified information. Both delegations, likewise, agreed that Qthe timing and contents of the first BISTF report of recommendations to the ministerial-level Security Consultative Committee (SCC) by October 31 -- will be discussed further at the next BISTF plenary in November in light of Japan's cabinet changes. Finally, the task force agreed to delay the establishment of a bilateral working group on standards and modalities for protecting classified shared information to late November to allow the Japanese government time to ensure that the proper mix of agencies are able to participate.
SCHIEFFER